Reliability Achievement Through the Technical Risk Assessment

Milena Krasich, P. E.
Jet Propulsion Laboratory, California 1 nstitute of Technology

Author

Milena Krasich is a Member of Technical Staff in the. Reliability Engineering Section of the Jet Propulsion Laboratory. She is a part-time professor at the California State University Dominguez I lills, teaching graduate courses in Reliability and Statistical Process Control, and at the California State Polytechnic University, Pomona, teaching undergraduate courses in Reliability, Environmental Testing, Production Systems Design, and Measurements. Milena holds an MS in Electrical Engineering from the University of Belgrade, Yugoslavia, and is a California registered electrical professional engineer. She is also a member of the IEEE and ASQC, and a fellow of the Institute of Environmental Sciences.

Introduction

To achieve a desired certainty in mission success with a minimum cost for the program, the Technical Risk Assessment was conceived as a management and design tool to identify, evaluate, and minimize the potentially high technical risk to spacecraft hardware.

Standard practice on JPL space programs has always been to identify the potential hazards through the Failure Mode and Criticality Analysis (FMECA), electrical circuits stress analysis, Worst Case Analysis (WCA), thermal management, testing at various product levels from the boards to the system level, and various other analyses. When a hazard was identified, the necessary improvements were made and verified, This standard practice, in view of cost restrictions, is more difficult to follow and implement. Therefore, up-front risk identification and reduction, along with the appropriately planned low cost test program, becomes a tool for cost vs. risk tradeoff. Program management through the technical risk assessment and tradeoff would minimize the cost of corrections and improvements by concentrating on the high risk drivers, while not spending the resources on the low or insignificant risks,

This paper concentrates on spacecraft technology, therefore, some of the identified risk drivers are specific to the industry. The methodology, however, the principles and the techniques can be extended to tit any program with non-repairable or repairable systems.

Abstract

In today's business and economic enviromnent, the primary goal of a manufacturer is to achieve the manufacture of a quality product with the minimum cost, reliability is thought of at the beginning of product development, in design, with the reliability vs. cost trade off using the technical risk assessment as a tool. A technique for reliability vs. cost tradeoff is being developed at JPL as a NASA sponsored project, the Technical Risk Assessment. The concept of this technique has been peer reviewed and is the topic of this paper.

Risk contributors (drivers) are identified for the specific product type. Many of the risk contributors are general, and can be related to any product, i. e., parts quality, design stress (worst case) analysis, test levels vs. use environment, radiation hardening or shielding vs. radiation environment, etc. The effect of each risk driver is then represented in a form of a mathematical algorithm, which is related to the desired for required mission reliability and cost. The highest un-reliability contributors are then evaluated to reduce the mission risk. The risk reduction cost of lower risk individual contributors is evaluated to address those that can be reduced with the least (or reasonable) cost to minimize overall spacecraft technical risk.
The technical risk assessment is designed to be used as a tool for risk identification and the assessment of the risk magnitude to enable an effective risk vs. cost tradeoff.

Kcy Words

Technical risk, risk reduction, tradeoff, reliability.

Background

The Technical Risk Assessment is a NASA sponsored project with a goal to identify spacecraft technical risk drivers and generate a tool for cost vs. risk tradeotT to achieve a reliable mission with the optimum cost by understanding the reliability of the spacecraft design in terms of the available resources expended or available prior to the design and launch. The concept was peer reviewed, and the detailed peer review of the individual algorithms is scheduled to take place in mid-year.

1. Specific reliabi 1 i t y considerate ions regarding spacecraft systems are as follows:
    - Spacecraft is a non-repairable system:
    - Mean Time Between Failures or Failure Density terms are not applicable,

2. Reliability values and topics of interest are:
    - Mission type, complexity, and duration,

8. Thermo-mechanical stress margin (test vs. flight)
9. Propellant or other consumables margin (supply vs. demand)
10. Radiation margin (environmental radiation dose distribution vs. part hardness
11. Dynamic stress margin, shock, vibration (test vs. flight)
12. Static stress margin (design vs. flight)
13. Analog interface margin, mechanical or electrical (source availability vs. load demand for electric power)
14. Solder attachment fatigue margin (flight thermal cycles vs. process qualification thermal cycles)
15. Environmental fatigue margin (expendable qualification units vs. protoflight units)
16. Residual un-corrected design faults
17. Electrical performance verification (WCA, pert stress, test)
18. Problem Failure Reporting, PFR, system; Red Flag design PFRs
19. Engineering unit availability
20. Residual urr-corrected workmanship defects
21. Quality control program (vendor and in-house), Red flag workmanship, material, process PFRs Pre-flight burn-in pmctices and stress screening (electrical and mechanical)
22. Inherited hardware
23. laihue-free test periods

Additional risk drivers that might be included in this study are

- Power Cycling Limited Life Equipment
- EMI protection
- Internal and external ESD prevention
- Hypervelocity impact on propulsion
- Adhesive joints
- Handling ESD protection of packaged electronics
- Limited life devices and reliability of design
- Fatigue life of propulsion components
- Inherited design solder joints thermal cycling

Individual risk factors can be divided in three basic types, based on their reliability analysis, as follows:

A. Time dependent (risk increases as a function of time)

- Hazard expressed as H(t)

B. Cycling-dependent (risk increases with the number of operational cycles)

- Hazard expressed as H(c)

C. Not dependent on time and/or cycling (pass or fail condition with one-shot devices)

- probability of failure represented by the binomial distribution;

D. Stress dependent

- Stress and strength assumed normally distributed
- Probability of failure is a standardized normal distribution with a design (stress) margin as a variable.

This paper offers examples for each of the risk categories.

A. Tin ie Dependent Risk Drivers

With the time-dependent risk drivers, risk increases with the elapsed time. A typical example would be part quality or part junction temperature, where part failure rate and consequently, the assembly failure rate increases with time. Using the Weibull Adjusted Probability of Survival, WAPS, conversion, hazard contributed by the increase in junction temperature is expressed as:

$$\Delta H_{JT}(t) = K(\beta)[\lambda(T)t^{\beta} - \lambda(T_B)]t^{\beta}$$

Where:

$K(\beta)$ = WAPS conversion (Reference 2)
$\lambda(T)$ = MIL-HDBK-2 17-predicted assembly failure rate at temperature T
$\lambda(T_B)$ = MIL-HDBK-2 17-predicted assembly failure rate at the reference (base) temperature, T_B.

Figure 2 shows failure rate multiplication as a function of junction temperature for a typical S/C assembly.

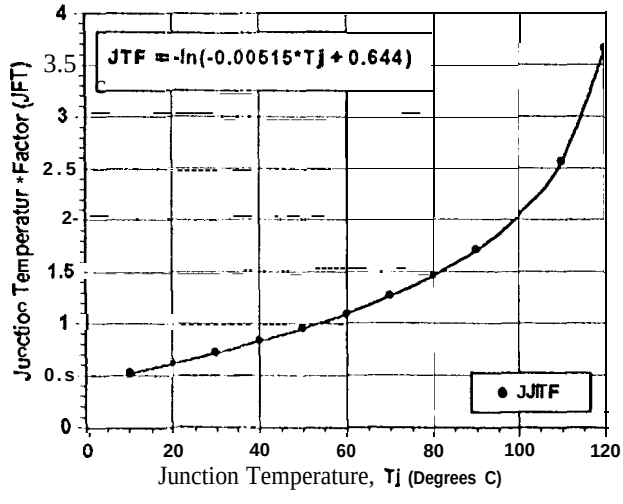

Figure 2. Multiplication Factor of the MIL-HDBK-217 - Predicted Failure Rate Calculated for a Typical S/C Assembly.

B. Cycling Dependent Risk Drivers

An example of risk introduced by cycling mechanical or electromechanical equipment is the assured reliability of cycling mechanisms through the cycling failure-free tests.

Here, a failure free test is defined as the test having a *failure free period of a predetermined duration that* is *achieved after the last recorded failure.*

In Figure 3, the ratio of the number of failure free test cycles to the mission required number of cycles is a part of the algorithm derived by the MATHCAD software. This is why the specific annotation was given to the x-axis.

C_T= Number of failure free test cycles

Ps = Probability that the test item will pass the test (usually given to be 0.96 or 0.97)

R_M = End-of-mission probability of survival

$$x = \ln(R_M)$$

$$p + z_{\alpha}\left[\frac{p\cdot(1-p)}{N}\right]^{\frac{1}{2}} \qquad \text{Hazard} = -x$$

Here, hazard is approximately equal to the probability of failure: $H \approx F$

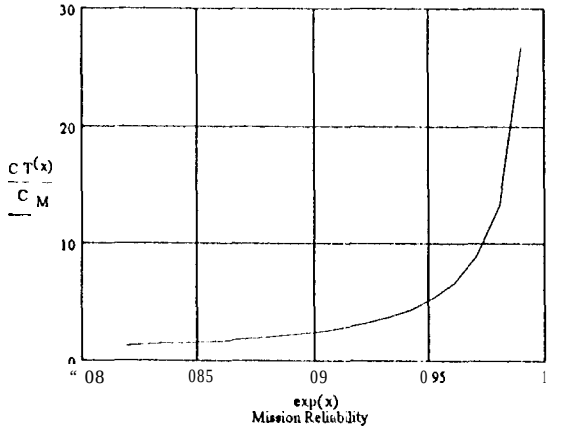

Figure 3. Ratio of Test Cycles vs. Expected Mission Cycles as a Function of Desired Mission Probability of Survival

C. Risk Drivers Non-Dependent of Time and/or Cycling; Discrete Risk Drivers

The discrete risk drivers are those found with one-shot devices, such as pyre-devices, opening or closing fixtures, etc. where the considered conditions are pass or fail.

Applicable distributions to the discrete risk driver-s are discrete distributions such as: binomial, hypergerometric, occasionally Poisson, etc. Reliability equation expressed as a binomial distribution is:

$$R = \sum_{k=r}^{n}\left(\frac{n!}{k!\,(n-k)!}\right)\cdot p_i^{k}\cdot(1-p_i)^{n-k}$$

Where

p_i = reliability of an individual item
r = number of failed items
n = total number of items

$$H = -\ln\left[\sum_{k=r}^{n}\left(\frac{n!}{k!\,(n-k)!}\right)\cdot p_i^{k}\cdot(1-p_i)^{n-k}\right]$$

To determine the fraction non-conforming:

The upper confidence limit on device probability of failure, p

(Binomial approximation to normal distribution)

Where

p = probability of a device failure, for no-failure tests,

$$p = \frac{1}{N}$$

N = sample size, nrrmbcr of devices tested,
Z_a = 0.68 for the standardized normal distribution with 50% confidence.
1 - *a* = percent confidence interval (50% confidence interval)

Reliability is:

$$R_0(N) = 1 - \left[\frac{1}{N} + Z_{\alpha}\left[\frac{\frac{1}{N}\left(1-\frac{1}{N}\right)}{N}\right]^{\frac{1}{2}}\right], \text{ or}$$

$$R_0(N) = 1 - \left[\frac{1}{N} + 0.68\left[\frac{1}{N^{\left(\frac{3}{2}\right)}}\cdot\sqrt{N-1}\right]\right]$$

Reliability of a redundant (parallel) pair of the one-shot devices is:

$$R_{parallel}(N, Z) = \frac{N^3 - N - 2\cdot\sqrt{N}\cdot Z_{\alpha}\cdot\sqrt{N-1} - Z_{\alpha}^{2}\cdot N + Z_{\alpha}^{2}}{N^3}$$

Hazard, being a negative natural logarithm of reliability is dependent on the number of units tested, but also on the desired confidence in the estimated value. Figure 4 shows hazard determined for a single one-activation device as a function of the number of tested units as well as the desired confidence. The higher level of confidence yields the higher hazard estimated values.

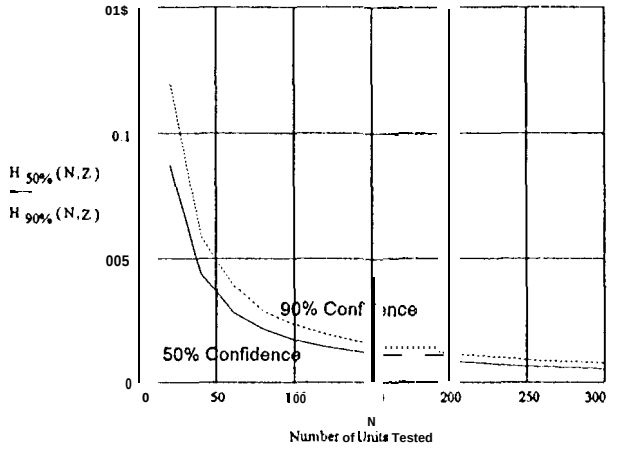

Figure 4. Hazard Assessed for a Single One-Shot Device as a Function of Number of Tested Devices and the Desired Confidence in Estimation

D. Stress-Dependent Risk Drivers

Stresses, such as environmental (climatic or dynamic, i. e., thermal, nuclear radiation, acoustic noise, etc.) or structural, affect components or spacecraft structure. Risk contributed by these drivers is compensated byensuringthsrt the spacecraft has enough of the design margin, and the required strength to endure the individual stresses. The S/C energy supply, such as propellant or electrical power, can be also viewed as stress/strength relationship.

To evaluate contributed risk the following assumptions are made:

- Stress and strength assumed normally distributed
- Reliability is a standardized normal distribution with a design (stress) margin, DM, as a variable.

$F(DM) \approx$ H(DM) = Area Under Both Curves

$$R(DM) = 1 - F(DM) = \Phi\left\{\frac{m-\mu}{(\sigma^2 + s^2)^{\frac{1}{2}}}\right\}$$

DM = Design Margin

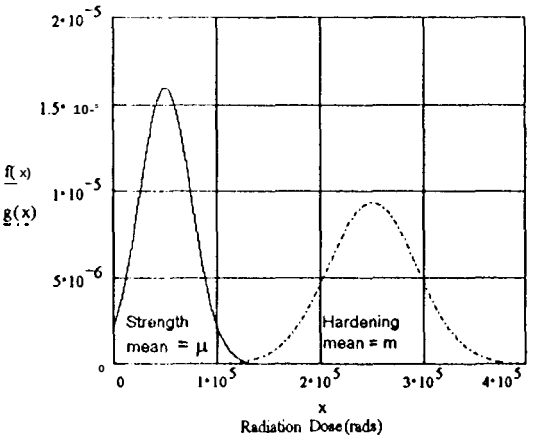

Figure 5. Radiation Environment and Hardening Distribution; Example

In the above graph:

F(DM) = probability of failure
R(DM) = reliability
μ = mean of the environment distribution
m = mean of the hardening distribution
f(x) = environment distribution,

g(x) = radiation hardening distribution

Risk is inversely proportional to the design margin, however, the assessment shows the magnitude of the design margin necessary for risk reduction. The technique can minimize the need or tendency for over-design.

Technical Risk Assessment, A Hypothetical Example

A hypothetical example is shown in Figure 6 to pictorially represents the technical risk assessment concept. The hypothetical practices in this example constitute of the following:

Parts quality used: Grade 11
Junction Temperatures: 85 °C
Electrical Stress: 60'%.
Duration of mission critical sequence: 7 days
Failure- free test of cycling devices: 5.3 times the mission number of cycles
One-actuation devices: 50 tested without failures
Thermo-mechanical stress margin: 20 'C
Radiation design margin: 1 RDM, 3 standard deviations,

The reference values are assumed to be:

Parts quality: Grade I
Junction Temper atures: 55 'C

Electrical stress: 50%
Mission critical sequence: None
Failure-free test of cycling devices: 27 times the number of mission cycles
One-actuation devices: 80 tested without failures
Thermo-mechanical stress margin: 30 'C
Radiation design margin: 2 RDM, 3 sigma

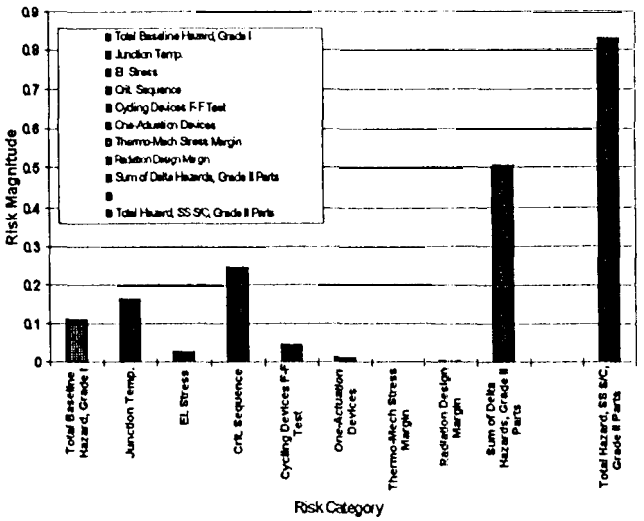

Figure 6. Technical Risk Assessment 1 Hypothetical Example of a Single String Spacecraft with Quality Grade II Parts

In the above example, the highs risk contributors would be the junction temperature and the mission critical sequence. Here, the critical sequence was considered to be a period of mission time when the spacecraft is autonomous, that is, there is no possibility of redundancy introduction via ground commands. The risk contribution of a critical sequence is also dependent on the percent of the spacecraft hardware redundancy dependent on the ground commands, or percent not autonomously redundant. The third significant risk contributor in the given example would be the insufficient testing of the cycling devices. The obvious conclusions drawn from the example would be to reduce the junction temperatures and to revise the mission so that the duration of the critical sequence is minimized. The next step in risk reduction would be to increase testing of the cycling devices for greater confidence in mission reliability, as well as to reduce electrical stress of the electronic devices.

Improvement of the radiation design margins or the thermo-mechanical stress margin in this example would constitute over-design and the unnecessary spending of the available resources.

Conclusions

The technical risk assessment is an attempt to quantify and correlate risks that result from various drivers specific to a certain mission and available practices and resources. Once quantified, relative to a specified baseline (usually the best achievable practice for a given technology), the highest risk contributors can be identified and addressed in a manner that is found to be reasonable and affordable. The technical risk assessment concept allows for cost effective reduction of the overall mission risk. It offers a valuable tool for risk-cost tradeoff and the respective appropriate management decisions.

The technique, being developed for a spacecraft, is adaptable to any other product by modification of existing, or creation of other related algorithms. When fully developed and modified for a specific application, the technical risk assessment will become an essential tool of a well managed and balanced limited-resource program

Acknowledgments

The research describedin this paper was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

The author of this paper wishes to express her special gratitude to the colleagues and peers who, with their technical expertise and comments have greatly contributed to the quality of the Technical Risk Assessment concept:

1. Dr. Steven Cornford, Jet Propulsion Laboratory
2. Mr. Roland Duphily, TRW
3. Mr. Thomas Gindorf, Jet Propulsion Laboratory
4. Mr. Howard Goldstein, Ames Research Center
5. Dr. Louie J. (Jack) Lipp, Department of the Army PM NBC Defense
6. Mr. James Marr, Jet Propulsion Laboratory
7. Mr. Seymour Morris (Program Manager, MIL-HDBK-217), Rome Laboratory, USAF
8. Mr. Harry Peacock, Jet Propulsion Laboratory (Retired)
9. Dr. Magdy Risk alla (Senior Staff Engineer), Voughd Aircraft Company
10. Mr. J. Charles Sawyer, NASA
11. Dr. JerrellStracener, Voughd Aircraft Company